PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/08, 7/10

A1

(11) International Publication Number: WO 99/53449

(43) International Publication Date: 21 October 1999 (21.10.99)

(21) International Application Number: PCT/IL99/00192

(22) International Filing Date: 6 April 1999 (06.04.99)

(30) Priority Data:
124008 8 April 1998 (08.04.98) IL

(71) Applicant *(for all designated States except US)*: ON TRACK INNOVATIONS LTD. [IL/IL]; Z.H.R. Industrial Zone, P.O. Box 32, 12000 Rosh Pina (IL).

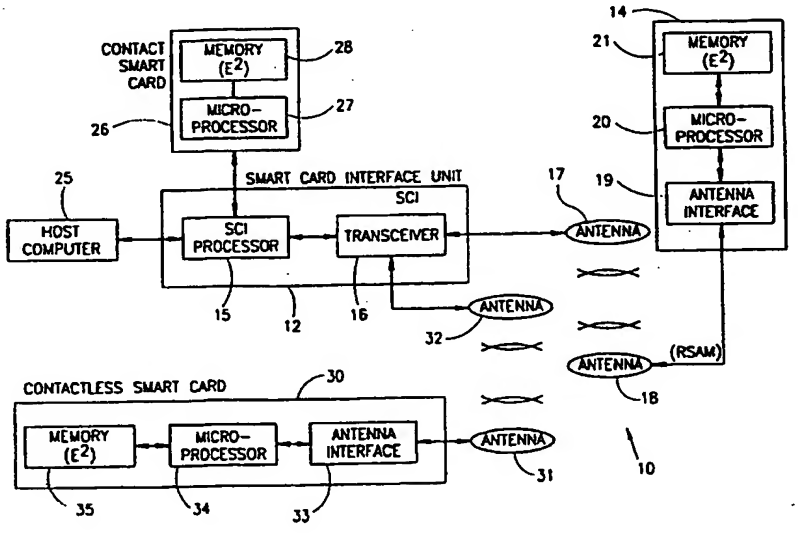
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: GILBOA, Ronnie [IL/IL]; Moshav Beit Hillel, 12255 Beit Hillel (IL). BASHAN, Oded [IL/IL]; Charzit Street 24, 20100 Carmiel (IL). ITAY, Nehemya [IL/IL]; Kibbutz Kfar Giladi, 12210 Kfar Giladi (IL). ADUK, Moshe [IL/IL]; Korazim 43, 12391 Korazim (IL).

(74) Agent: REINHOLD COHN AND PARTNERS; P.O. Box 4060, 61040 Tel Aviv (IL).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURED DATA TRANSACTION SYSTEM FOR SMART CARDS



(57) Abstract

A secured data transaction system (10) comprising a Smart Card Interface (SCI) (12) for interfacing between a local device (25, 26) and a Remote Secure Application Module (RSAM) (14) located remote from the SCI for processing data from smart cards. The SCI (12) comprises an SCI memory (28, 35) containing a predetermined instruction set, an SCI processor (15) coupled to the memory for operating in accordance with said instruction set, and a first SCI communication interface (16) coupled to the SCI processor for allowing bi-directional contactless communication between the SCI and the RSAM. The RSAM (14) comprises an RSAM memory (21) containing a predetermined instruction set and comprising a secured area reserved for security applications and for secure storage of data related thereto, an RSAM processor (20) coupled to the RSAM memory for operating in accordance with said instruction set, and an RSAM communication interface (19) coupled to the RSAM processor for allowing bi-directional contactless communication between the RSAM and the SCI. In such an arrangement data associated with the smart card interface (12) may thus be stored in the RSAM memory (21) remote from the smart card interface.

Secured data transaction system for smart cards

FIELD OF THE INVENTION

This invention relates to a data transaction system for smart cards and, in particular, to a secured data transaction system where the transactions and the data related thereto are securely stored.

BACKGROUND OF THE INVENTION

Smart cards are becoming increasingly important and widespread for all manner of data transactions. Typically, a smart card user performs a transaction via a read/write station containing a user interface, a card interface and a processor with a memory. To perform a transaction with a smart card, the user defines his request via the card interface, which feeds data to the processor for execution and storage in memory. The results of such a transaction are usually stored as data in the memory of the station for later use. In practice, data retrieval generally takes place either at a time convenient to the resources of the system, or on a periodic basis. Later on, the institution involved in the deal may retrieve the data and credit or debit the user's account, as appropriate.

Methods of practical implementation of security measures are taught, for example, in US Patent 5,664,017 in the name of Gressel *et al.* and in US Patent 5,694,472 for a Personal Management System to Johnson *et al.*

Since relatively large sums of money may be involved, transaction information is of great value both to the user of the card and to the company concerned. Therefore, it is important to safeguard the data against possible loss, such as loss due to a power shortage. One known approach that provides a partial remedy is the use of non-volatile memories, able to retain data even without power. Nevertheless, even non-volatile memory cannot prevent physical damage incurred by the read/write station from the possible destruction of the stored data.

Another conventional measure for the prevention of potential loss of data in memory is immediately to transfer the data out of memory, for real-time processing. However, although feasible, this kind of response imposes a strain on the communication and processing resources by requiring attention without delay, thus increasing costs to the provider of the service and, ultimately, to the customer. It would thus be advantageous if data could be left in memory without fear of loss resulting from possible damage suffered by the card read/write station.

Besides physical harm to the data card station, there is also the danger of an electrical malfunction, even as unintentional as a mistake by personnel performing routine maintenance. For example, an accidental short-circuit due to human error is enough to wipe out the contents of a memory device. Therefore, isolation of the memory from electrically conductive connections is desirable.

For mobile card reader systems, such as those to be installed for fare collection in vehicles of mass transportation services, there lingers the peril of an accident destroying the data transaction equipment, including memory and data. It would therefore be beneficial to provide for crash-proof protection to

the RSAM comprising:

an RSAM memory containing a predetermined instruction set and comprising a secured area reserved for security applications and for secure storage of data related thereto,

an RSAM processor coupled to the RSAM memory for operating in accordance with said instruction set, and

an RSAM communication interface coupled to the RSAM processor for allowing bi-directional contactless communication between the RSAM and the SCI;

whereby data associated with the smart card interface is stored in the RSAM memory remote from the smart card so as to be inaccessible to or from the smart card.

Thus in accordance with the invention, the security measures and secured operations and their storage are assigned to a remote device separate from the read/write station accepting the smart cards. A read/write station, constituted by the Smart Card Interface or SCI, receives the smart card and forwards the data stored therein to the Remote Secured Application Module, (RSAM), for processing the security measures and the transactions and for storing the security measure software, the transactions and the data related thereto.

It follows that to prevent the loss of data stored in memory in case of complete or partial damage to the station, the memory device is best maintained separate from the read/write station. Thus, by confining the data memory as a separate entity in its own housing, detached from the read/write station, the chances are high that the data will remain intact regardless of harm to the station.

Further security may be achieved by hiding the memory device containing the data, so as to render it less easily accessible. Alternatively, security may be enhanced by preventing the physical removal of the memory

authorizes data retrieval from the RSAM and commands secure storage of data received from the RSAM memory into the host memory.

BRIEF DESCRIPTION OF THE DRAWINGS

In order to understand the invention and to see how it may be carried out in practice, a preferred embodiment will now be described, by way of non-limiting example only, with reference to the accompanying drawings, in which:

Fig. 1a is a block diagram showing functionally a detail of a secure data transaction system according to a first embodiment of the invention;

Fig. 1b shows schematically a modification to the system shown in Fig. 1a;

Fig. 2a and 2b show schematically further variations of the system illustrated in Figs. 1a and 1b; and

Fig. 3 is a flow diagram showing the principal operating steps associated with the system shown in Fig. 1a.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Fig. 1a shows a system designated generally as 10 comprising a Smart Card Interface (SCI) 12, and a Remote Secured Application Module (RSAM) 14. The SCI 12 may be part of a station such as, for example, an Automatic Teller Machine (not shown in Fig. 1a), utilized for reading and for writing to secured contact/contactless smart cards for carrying out financial transactions. The SCI 12 includes a processor 15 (constituting an SCI processor) coupled to a transceiver 16 having a coil antenna 17 for effective non-contact inductive coupling with a coil antenna 18 coupled to the RSAM 14. The SCI 12 is energized by an external power supply whilst the RSAM 14 may or may not be self-powered, as will be explained in greater detail below.

memory 35 may be an EEPROM operating in similar manner to the EEPROM 21 in the RSAM 14 so as to allow customization of the antenna interface 33.

In such an arrangement the transceiver 16 is a first SCI communication interface for allowing bi-directional contactless communication with the contactless smart card 30, whilst the processor 15 constitutes a second SCI communication interface for allowing bi-directional contact communication with the contact smart card 26 and with the local device 25. If desired, a separate contactless interface may be coupled to the processor 15 for allowing for contactless communication with the local device, be it a host computer or another smart card.

Although data is stored securely in the RSAM 14, authorized parties may retrieve stored data from the RSAM by means of the SCI 12. In the event of a malfunction of the SCI 12 preventing retrieval of data from the RSAM 14, the malfunctioning SCI 12 may be replaced by another functional SCI 12.

Fig. 1b shows schematically such a system comprising two identical SCIs, 12 and 12′, each in close contactless communication with the RSAM 14. The SCI 12′ constitutes an auxiliary SCI which may be used temporarily for the purpose of data retrieval only or as a substitute for the malfunctioning SCI 12 until a replacement is installed. Alternatively, both the SCIs 12 and 12′ may be permanently installed and configured for alternate operation, or the system may be configured so that the SCI 12 perform transactions while the SCI 12′ retrieves data from the RSAM 14. Since both of the SCIs 12 and 12′ are identical, their tasks may be interchanged.

Fig. 2a shows schematically yet another arrangement wherein the three elements SCI 12, SCI 12′ and RSAM 14 form a group in which the elements are mutually remote from each other. Besides being separate, the communication between the RSAM 14 and either of the SCIs 12 or 12′ is contactless. Both the remoteness and the contactless communication ensure that a failure

Communication and energy transfer between the SCI 12 and the RSAM 14 is via inductive coupling in accordance with the teachings of US Patent 5,241,160 entitled "A System and Method for the Non-Contact Transmission of Data", in the name of Bashan *et al.*, incorporated herein by reference. This patent also explains how the impedance of a cable connecting a coil antenna to a transmitter may be varied without requiring re-tuning of the card resonant frequency.

Using these techniques, the matched coil antenna of the SCI may be connected by a length of SCI cable to the SCI 12 and the SCI cable may be deployed outside of the SCI so that it may be brought close to the tuned coil antenna of the RSAM 14. The distance between the SCI 12 and the RSAM 14 may thereby be significantly increased.

In like manner, the tuned RSAM coil antenna may also be connected to the RSAM 14 by a length of RSAM cable that may extend out of the housing of the RSAM. Moreover, both the SCI cable and the RSAM cable may be extended so that the maximum distance between the SCI 12 and the RSAM 14 is equal to the combined length of both cables. It will be appreciated that either or both of the two coil antennas may be connected via respective cables of equal or unequal lengths.

The length of the coil antenna cable is preferably determined as multiples of half-wavelengths, starting from zero for up to eight half-wavelengths. The measured length of such a coil antenna cable depends therefore on the frequency of the carrier signal used. Thus, assuming a carrier frequency equal to 13.56 MHz, one half-wavelength, taking the influence of the cable into account, amounts to 8 m. Preferably the length of the coil antenna cable will not reach more than 48 m and ideally it should be less than 32m. The aforementioned U.S. Patent 5,241,160 lists the factors influencing the relative distance allowed between the two coil antennae and provides information about the distances obtainable.

is decrypted by the RSAM so as to authenticate the card. If authentic, then the encrypted Account Certificate is also decrypted so as to produce an encrypted Transaction Certificate. This is fed, via non-contact communication to the SCI from where it is forwarded to the card via contact or non-contact communication. The card now decrypts the transaction data is so as to authenticate the RSAM. If authentic, the transaction is processed and an encrypted Settlement Certificate is prepared for feeding via contact or non-contact communication back to the SCI from where it is forwarded via non-contact communication to the RSAM wherein the transaction data is again decrypted so as to authenticate the card. If authentic, then the purse account is settled. In the event of an invalid card or RSAM, the transaction is aborted and a suitable message relayed via the SCI.

Whilst preferred embodiments of the invention have been described in detail, it is apparent that many modifications and variations thereto are possible, all of which fall within the scope of the invention as defined in the appended claims.

Thus, for example, whilst in the preferred embodiment a matched antenna is employed in the SCI, it will be understood that a conventional resonant circuit may be employed as is well known in the art.

3. The secured data transaction system according to Claim 1 or 2, further including an auxiliary SCI (12') for allowing parallel or backup data retrieval from the RSAM memory.

4. The secured data transaction system according to any one of the preceding Claims, wherein the Smart Card Interface includes a second SCI communication interface (15) for allowing bi-directional communication with the local device.

5. The data transaction system according to any one of the preceding Claims, wherein:

the RSAM contains security means for prevention of unauthorized transactions and unauthorized access to RSAM functions and RSAM memory.

6. The data transaction system according to any one of the preceding Claims, wherein:

the SCI communication interface (16) communicates with a smart card and the RSAM by contactless inductive coupling communication.

7. The data transaction system according to Claim 6, wherein:

the first SCI communication interface (16) is coupled to an SCI coil antenna (17) operating at a predetermined frequency, and

the RSAM communication interface (19) is coupled to an RSAM coil antenna (18) tuned to said predetermined frequency.

8. The data transaction system according to Claim 7, wherein the first SCI communication interface is coupled to the SCI coil antenna (17) by an SCI cable having a length which may be varied without requiring the first SCI communication interface to be re-tuned to said predetermined frequency.

9. The data transaction system according to Claims 7 or 8, wherein the RSAM communication interface (19) is coupled to the RSAM coil antenna (18) by a cable.

an RSAM communication interface (19) connected to the RSAM processorfor bi-directional inductive coupling communication with at least one SCI, and

a data card for containing the RSAM therein, the data card being remote from the SCI;

whereby the SCI transfers data exchanges between secured smart cards and the RSAM, the RSAM providing for the secured processing of transactions and the RSAM also providing a secured repository for the transactions and for data related thereto.

16. The data transaction system according to any one of the preceding claims, wherein the SCI also provides energy for functions of the RSAM thereby obviating the need for the RSAM to be self-powered.

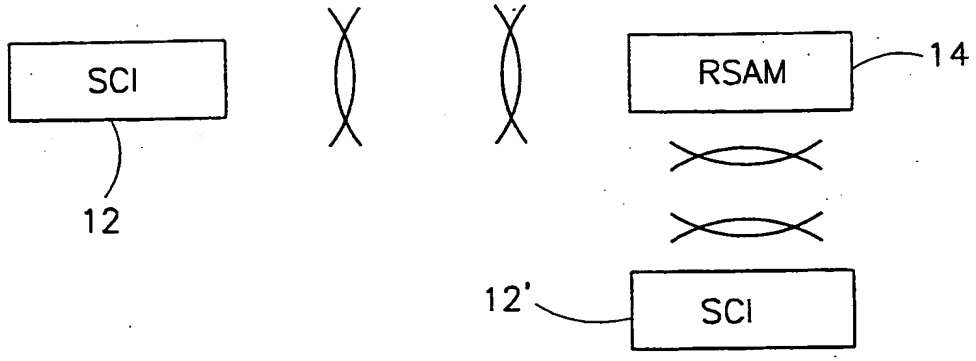


FIG.1B

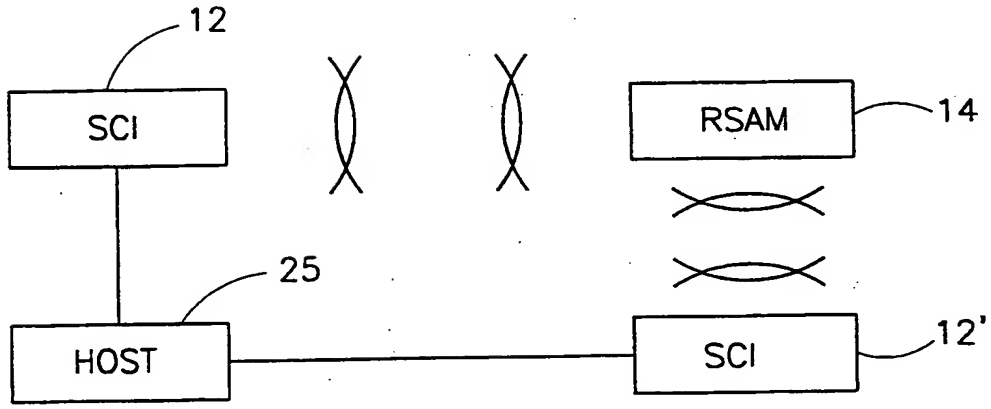


FIG.2A

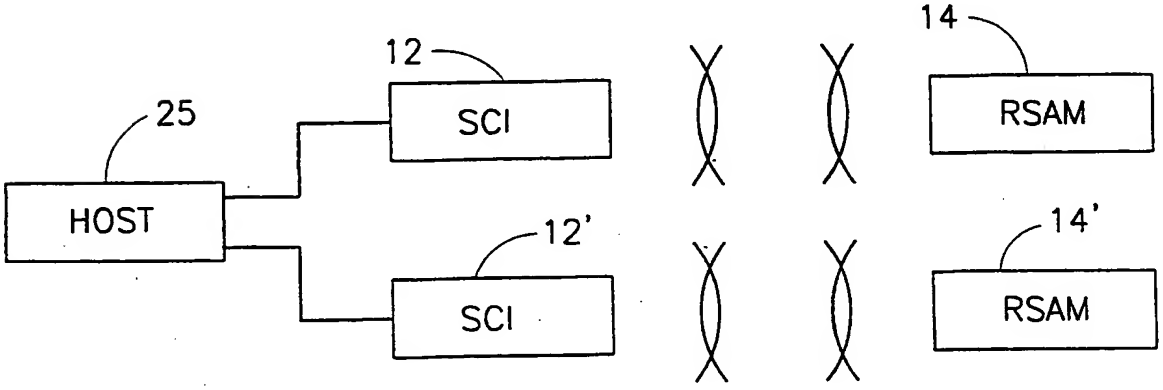


FIG.2B

INTERNATIONAL SEARCH REPORT

Ir ational Application No
PCT/IL 99/00192

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/08 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 572 004 A (RAIMANN GERHARD) 5 November 1996 (1996-11-05)	1-5,15
A	column 2, line 19 - line 23 column 2, line 50 - line 55 column 3, line 4 - line 26 column 3, line 46 - line 55 column 3, line 64 - column 4, line 2; figures 1,2 abstract	6,16

Y	FR 2 740 291 A (SAGEM) 25 April 1997 (1997-04-25)	1-5,15
A	page 1, line 26 - line 33 page 2, line 12 - line 20 page 5, line 8 - line 30; figures 1,3 abstract	7-11,15, 16

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 1999	13. 09. 1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Wauters, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

nformation on patent family members

In ational Application No
PCT/IL 99/00192

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5572004 A	05-11-1996	AT 161348 T	15-01-1998
		DE 59307854 D	29-01-1998
		EP 0600170 A	08-06-1994
FR 2740291 A	25-04-1997	NONE	
US 5241160 A	31-08-1993	AT 173103 T	15-11-1998
		AU 640843 B	02-09-1993
		AU 9001191 A	02-07-1992
		CA 2058330 A	29-06-1992
		DE 69130447 D	10-12-1998
		DE 69130447 T	01-07-1999
		EP 0492569 A	01-07-1992
		ES 2125860 T	16-03-1999
		IL 100451 A	26-08-1994
		SG 46663 A	20-02-1998
EP 0534559 A	31-03-1993	NL 9101608 A	16-04-1993
		JP 5307655 A	19-11-1993
US 4849927 A	18-07-1989	GB 2205667 A	14-12-1988
		CA 1288492 A	03-09-1991
		DE 3818960 A	22-12-1988
		FR 2616561 A	16-12-1988
		JP 63317862 A	26-12-1988
GB 2079504 A	20-01-1982	NONE	